

47

Notice of Allowability

Application No.

09/673,137

Examiner

Minh Dinh

Applicant(s)

PINKAS, DENIS

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment filed 1/31/2005 and examiner's amendment on 4/25/2005.
 2. ☒ The allowed claim(s) is/are 7-12.
 3. ☒ The drawings filed on 31 January 2005 are accepted by the Examiner.
 4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☒ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
- * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☒ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☒ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|--|---|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input checked="" type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. |
| 3. <input checked="" type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____. |

EXAMINER'S AMENDMENT/COMMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Jason Vick on 4/25/2005. The application has been amended as follows:

Amendments to the Specification:

Page 14:

Please substitute the following paragraph for the paragraph beginning at line 18:

Fig. 4b represents a structure of a completed request message, for example in a format in accordance with the aforementioned ~~ANSI~~ ASN1 coding. In this case, the coding of these messages is performed in accordance with the so-called TLV mode, in which T designates the type of the field, L the length of the latter and V the value of the field.

Please substitute the following paragraph for the paragraph beginning at line 22:

Fig. 4b, at point 1), represents the structure of a certification request template GRCA in such a case, which is considered to be formed by a set of fields TLV that are sequential or interleaved in accordance with the ~~ANSI~~ ASN1 standard. This request template is formed outside the embedded system. It must include, and this is verified by the embedded system, three fields and three fields only, which correspond to: 1) a type of algorithm identifying field, 2) a type of public key value field, 3) a type of public key usage indicator field. The position of each of these fields among the other fields of the request template must also correspond to a precise position, i.e. it must be preceded and followed by predetermined different types of fields.

Amendments to the Claims:

Claims 1-6 (Cancelled)

7. (Previously Presented) A method for verifying the usage of public keys of a set of asymmetric keys, a public key (K_p) and private key (K_s) generated for a given use, such as encryption/decryption or digital signature verification/generation, by an on-board system and stored in the storage area of the on-board system (S_i) equipped with cryptographic calculation means and externally accessible read/write-protected means for storing digital data, said digital data (ID_d_i) comprising at least a serial number (SN_i) for identifying the on-board system and an identification code (Op_j) of an operator authorized to configure said on-board system, a request being formulated by said on-board system by transmitting a request message (MRCA) containing said public key (K_p) to a certification authority (CA), comprising:

PRIOR TO ANY TRANSMISSION OF A CERTIFICATION REQUEST, DURING THE CONFIGURATION OF A SET (L_k) OF ON-BOARD SYSTEMS (S_i) BY THE AUTHORIZED OPERATOR:

- generating by the authorized operator, for said set of on-board systems, a mother public key (K_{pM}) and a mother private key (K_{sM}) used in connection with a process supported by an algorithm (CA1M);

- publishing said mother public key (KpM) associated with the algorithm ($CAIM$), the identification code of said authorized operator (OP_i), and defining a range of on-board system identifiers for the set (Lk) of on-board systems;
- calculating, for each on-board system of said set (Lk) of on-board systems, from said mother private key (KsM) and from the serial number (SN_i) of the on-board system, a diversified private key ($KsMi$), and storing said diversified private key ($KsMi$) in said externally accessible, read/write-protected storage area, and;

PRIOR TO ANY TRANSMISSION OF A CERTIFICATION REQUEST MESSAGE:

- generating by the on-board system a certification request (RCA) containing, in particular, a field of the public key (Kp) and usage indicators (U) of said public key,
- using said calculation means and said diversified key ($KsMi$) associated with this on-board system to calculate a cryptographic control value (Sc_i) on the entire request (RCA), said cryptographic control value being a digital signature calculated by means of the diversified private key ($KsMi$);

WHEN A CERTIFICATION REQUEST IS SENT TO THE CERTIFICATION AUTHORITY BY THE ON-BOARD SYSTEM:

- forming a certification request message (MRCA) containing the request (RCA), the identifier (IDd_i) of the on-board system, the request message being constituted by the identification code (OP_i) of this authorized operator and by the serial number (SN_i) of the on-board system, and a cryptographic control value (Sc_i);
- transmitting to the certification authority (CA) said request message (MRCA) formed during the preceding phase and containing the public key (Kp) and the usage indicators (U) subject to said certification, and said cryptographic control value (Sc_i);
- and

WHEN A CERTIFICATION REQUEST MESSAGE (MRCA) IS RECEIVED BY THE CERTIFICATION AUTHORITY:

- retrieving the identification code of the authorized operator (OP_j) from the digital data (IDd_i) of the on-board system,
- retrieving, from said identification code (OP_j) of said authorized operator, the value of the mother public key (KpM) as well as the identifier of the algorithm (CA1M) associated with the set (Lk) of the on-board system,
- verifying, from said mother public key (KpM), from said serial number (SN_i) of the on-board system, and from said certification request message (MRCA) received, said cryptographic control value (Sc_i), and establishing the authenticity of said cryptographic control value and the source of this certification request.

8. (Previously Presented) A method according to claim 7, characterized in that when the certification request (RCA) is generated by the on-board system, the method further comprises generating, at the on-board system level, a certification request (RCA), composed of three fields, including a public key algorithm identifier (CA1), a public key value (Kp), and an indicator of the usages of said key (U).

9. (Previously Presented) A method according to claim 7, characterized in that when the certification request is completed by the on-board system, the method further comprises the step of communicating a certification request template (GRCA) to said on-board system;

- checking, at the on-board system level, the syntax of the certification request template (GRCA) to ensure that it is a correctly formed certification request, and

- conditioning a step consisting of having the on-board system fill in missing fields of the certification request template (GRCA) to a positive verification.

10. (Previously Presented) A method according to claim 7, characterized in that, for a set of asymmetric signature keys (Kp), (Ks) generated by said on-board system, allowing use of the private key (Ks) under control of the cryptographic calculation means only for signature generation purposes, said private key (Ks) stored in said externally accessible read/write-protected storage area being unknown to the user and limited to a utilization exclusively for digital signature purposes, the utilization of said key being limited to signature purposes and the utilization of the certificate containing the corresponding public key being limited to signature verification purposes.

11. (Previously Presented) A method according to claim 7, characterized in that for a set of asymmetric keys, a public asymmetric encryption key (E_p) and a private asymmetric decryption key (D_s) generated by said on-board system, the method consists of associating, with said encryption and decryption keys (E_p), (D_s) and with the asymmetric decryption process, a symmetric "weak" decryption process and key, the symmetric decryption key being encrypted, then decrypted, by means of the private asymmetric decryption key (D_s), said private key (D_s) stored in said externally accessible read/write protected storage area being unknown to the user, so as to authorize the utilization of said key only for weak decryption purposes, the utilization of the certificate containing the corresponding public key being limited to said weak encryption purposes.

12. (Currently Amended) An on-board system comprising a card having a microprocessor, a RAM, a nonvolatile memory including a programmable memory and an externally accessible protected storage area memory, a cryptographic calculation module and an input/output system connected by a link of the BUS type,

- a diversified private key K_{sM} , stored in said externally accessible protected memory, said diversified private key, being unique and distinct for said on-board system and calculated from a mother private key K_{sM} and an identification number of said on-board system, and being further associated with a mother public key K_{pM} ;

- said cryptographic calculation module comprising:

- means for calculating a signature from said diversified private key KsM_i , making it possible to calculate the signature of a certification request to certify a public key Kp associated with a private encryption key Ks or signature key, respectively, said private key Ks generated by said signature calculation means being stored in said externally accessible protected memory, said signature of the certification request being a function of the identification number of said on-board system and an identification code of an authorized operator, said signature calculation means making it possible to transmit to a certification authority a certification request message containing said certification request and said signature, which allows said certification authority to verify the source of the certification request from said on-board system and the protection of said diversified private key and private signature key in said externally accessible protected memory using only public elements, such as said mother public key KpM .

2. Corrected drawings filed 1/31/2005 are approved. Formal drawings are required.
3. The substitute declaration filed 1/31/2005 is deficient. The declaration is defective because: (a) the PCT International Application number is not correct; and (b) it was signed on 2/14/2005, which came after the filing date. Correction is required.
4. The following is an examiner's statement of reasons for allowance. The present invention is directed to a method for requesting a public-key certificate using a cryptographic module. More specifically, independent claims 1 and 12 identify the uniquely distinct features: the private key of the cryptographic module used to sign a

certification request is a diversified private key calculated from a mother private key and the serial number of the cryptographic module, and that the certification request includes an identification code of an authorized operator and the ID number of the cryptographic module. The closest prior art, Matyas (5,164,186), discloses a method for requesting a public-key certificate using a cryptographic module. Other prior art teaches generating a diversified private key (Austin/4,944,007), generating a key using a user's identifying information ID (Yuval/5,586,186) and associating a key with an identification code of an authorized operator (Pauschinger/6,041,704). However, Matyas, Austin, Yuval and Pauschinger, either singly or in combination, fail to teach that the private key of the cryptographic module used to sign a certification request is a diversified private key calculated from a mother private key and the serial number of the cryptographic module, and that the certification request includes an identification code of an authorized operator and the ID number of the cryptographic module. The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claimed invention is therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
4/27/05


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100